AMENDMENTS TO THE CLAIMS

1. - 20. (Canceled)

21. (New) A system for tracing content in a highly distributed system, comprising:

a plurality of network devices, wherein each network device in the plurality is configured to perform actions, comprising:

receiving encrypted content associated with a content owner in the highly distributed system;

determining if the received content is to be decrypted;

if the received content is to be decrypted:

decrypting the received content,

determining a self-identifier that uniquely identities the current network device in the plurality of network devices, and

modifying the decrypted content by embedding at least one of a fingerprint or a watermark into the decrypted content, wherein the fingerprint or watermark is generated, in part, from the self-identifier; and

if the decrypted content is to be provided to another network device in the plurality of network devices:

encrypting the modified content;

wrapping the encrypted modified content together with the self-identifier using an access key; and

providing the wrapped encrypted modified content to the other network device in the plurality of network devices.

22. (New) The system of claim 22, wherein each network device in the plurality of network devices is further configured to perform action, further comprising:

if the received encrypted content is to be provided to another network device in the plurality of network devices absent decrypting the received encrypted content, providing the received encrypted content to the other network device in the plurality of network devices.

23. (New) The system of claim 22, wherein decrypting the received encrypted content further comprises:

obtaining a different access key out-of-band, wherein the different access key is uniquely associated with the network device currently having decrypted the content and a sending network device of the content to the current network device in the plurality of network devices; and

employing the different access key to unwrap the received content before decrypting the received content.

24. (New) The system of claim 22, wherein the self-identifier further comprises at least one of a serial number, and a time stamp indicating approximately when the content is decrypted.

25. (New) The system of claim 22, wherein the set of information further comprises at least one of traceability information, a time stamp, an identifier, and registration information associated with at least one of the content and the current network device in the plurality of network devices.

26. (New) A network device in a plurality of network devices for managing content in a highly distributed system, wherein each network device comprises:

a transceiver that is arranged to receive and to send content to another network device in the plurality of network devices; and

a processor that is configured to execute program code that performs actions, including:

receiving encrypted content in the highly distributed system;

determining if the received content is to be decrypted, and if the received content is to be decrypted:

decrypting the received content,

determining a self-identifier that uniquely identities the current network device in the plurality of network devices, and

modifying the decrypted content by embedding at least one of a fingerprint or a watermark into the decrypted content, wherein the fingerprint or watermark is generated, in part, from the self-identifier; and

if the decrypted content is to be provided to another network device in the plurality of network devices:

encrypting the modified content;

wrapping the encrypted modified content together with the self-identifier using an access key; and

providing the encrypted modified content to the other network device in the plurality of network devices.

27. (New) The network device in a plurality of network devices of Claim 26, wherein at least one of the network devices is managed by at least one of a content owner, a content aggregator, a service operator, or an end-user.

28. (New) A method for tracing content in a highly distributed system, comprising:

for each network device in a plurality of network devices along the highly distributed system:

receiving encrypted content by a current network device in the plurality of network devices in the highly distributed system;

determining if the received content is to be decrypted, and if the received content is to be decrypted:

decrypting the received content,

determining a self-identifier that uniquely identities the current network device in the plurality of network devices, and

modifying the decrypted content by embedding at least one of a fingerprint or a watermark into the decrypted content, wherein the fingerprint or watermark is generated, in part, from the self-identifier for the current network device; and

if the decrypted content is to be provided to another network device in the plurality of network devices:

encrypting the modified content;

wrapping the encrypted modified content together with the self-identifier using an access key; and

providing the encrypted modified content to the other network device in the plurality of network devices.